DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Applicant's submission filed on July 14th, 2008, has been entered.

2. Claims 1-18 have been presented for examination and are rejected.

Response to Arguments

3. Applicant's arguments filed July 14th, 2008, with respect to the claims have been considered but are moot in view of the new grounds of rejection.

Terminal Disclaimer

4. The terminal disclaimer filed on July 14th, 2008, disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of the full statutory term of prior application No. 09/626,577 has been reviewed and is accepted. The terminal disclaimer has been recorded. The provisional double patenting rejection of claims 1-18 is withdrawn.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 6, 10, and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically,

a. Claim 6 recites "the compression" without proper antecedent basis.

b. Claim 10 recites "the comparisons" and is dependent on claim 9, which appears to describe only one comparison (i.e., comparing the first and second digital fingerprints). Similarly, dependent claim 12 refers to comparison in the singular form.

c. Claim 18 recites "the comparison" without proper antecedent basis.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-18 rejected under 35 U.S.C. 102(b) as being anticipated by Tomkow (WIPO Publication No. WO 01/10090 A1, published February 8th, 2001).

9. As per claim 1, Tomkow teaches a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender, (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

adding a pixel for indicating the opening of the message at the recipient to the message at the server, transmitting the message from the server to the recipient, the message including the pixel for indicating the opening of the message at the recipient, (Tomkow, pg. 12, lines 13-28 overview; see, e.g., implementation details of pg. 13, line 19, to pg. 14, line 31)

transmitting the message from the recipient to the server, including the pixel for indicating the opening of the message at the recipient, when the message is opened at the recipient, providing an encrypted hash of the message, including the indication of the opening of the message at the recipient, at the server, and transmitting the message, including the indication of the opening of the message at the recipient, and the encrypted hash to the sender (Tomkow, see pg. 22, line 14 to pg. 25, line 2, including the creation of an encrypted hash of the message with an indication of the opening of the message at the recipient; see also figs. 2E and 2F).

10. As per claim 2, Tomkow teaches the system further including the steps at the server of:

receiving at the server the message, including the indication of the opening of the message at the recipient and the encrypted hash of the message, and determining the authenticity of the message, including the opening of the message at the recipient, on the basis of the hash of the message, including the indication of the opening of the message at the recipient, and the hash decrypted from the encrypted hash (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7 validation process where the message is received at the server).

11. As per claim 3, Tomkow teaches the system further including the steps at the server of: receiving from the sender the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, hashing the message, including the indication of the opening of the message at the recipient, to provide a first digital fingerprint of the message including the indication of the opening of the message at the recipient, decrypting the encrypted hash of the message, including the indication of the message at the recipient, to provide a second digital fingerprint of the message including the indication of the opening of the message at the recipient, and comparing the first and second digital fingerprints to determine the authenticity of the message including the indication of the opening of the message at the recipient (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7 validation process where the message is received at the server, including where a first and second digital fingerprint of the message are created).

12. As per claim 4, Tomkow teaches the system further including the steps at the server of:

indicating to the sender the results of the comparison, and disposing of the message, and including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the message at the recipient, when the message and the encrypted hash are transmitted by the server to the sender (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

13. As per claim 5, Tomkow teaches the system further wherein the server receives the message from the sender through the internet, the server transmits the message to the recipient through the internet, the server receives the message, including the indication of the opening of the message at the recipient, through the internet, and the server transmits the message, including the indication of the opening of the message at the recipient, through the internet to the sender (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1).

14. As per claim 6, Tomkow teaches the system further wherein the server indicates the results of the compression to the sender through the internet and wherein the server disposes of the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the

opening of the message, when the message and the encrypted hash are transmitted by the server to the sender through the internet (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

15. As per claims 7 and 13, Tomkow teaches a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

receiving the message at the server from the sender, transmitting the message from the server to the recipient through a network including at least one interim network station unknown to the sender at the time the message is transmitted, (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

the message including a pixel for indicating the opening of the message at the recipient, (Tomkow, pg. 12, lines 13-28 overview; see, e.g., implementation details of pg. 13, line 19, to pg. 14, line 31)

receiving the message, including the indication of the opening of the message the recipient, at the server, (Tomkow, see pg. 22, line 14 to pg. 25, line 2).

receiving an attachment at the server including an indication of the interim network stations which receive the message during the transmission of the message from the server to the recipient and back to the server, (Tomkow, see, e.g., pg. 5, lines 6-33 and pg. 22, line 14 to pg. 25, line 2, where the interim network stations are recorded and attached)

providing encrypted hashes of the message, including the indication of the opening of the message at the recipient, and the attachment, and transmitting to the sender the message, including the indication of the opening of the message the recipient, and the attachment, and the encrypted hashes of the message, including the opening of the message at the recipient, and the attachment (Tomkow, see pg. 22, line 14 to pg. 25, line 2, including the creation of an encrypted hash of the message with an indication of the opening of the message at the recipient; see also figs. 2E and 2F).

16. As per claim 8, Tomkow teaches the system further including the steps at the server of:

receiving at the server the message, including the indication of the opening of the message at the recipient, the attachment and the encrypted hashes of the message, including the indication of the opening of the message at the recipient, and the attachment, and determining the authenticity of the message, including the opening of the message at the recipient, on the basis of the hash of the messages, including the indication of the opening of the message at the recipient, and the hash decrypted from the encrypted hash and the authenticity of the attachment on the basis of the hashed attachment and the hash decrypted from the encrypted hash of the attachment (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

17. As per claims 9 and 15, Tomkow teaches the system further including the steps at the server of:

reviewing from the sender the message, including the indication of the opening of the message at the recipient, the encrypted hash of the message, including the indication of the opening of the message at the recipient, the attachment and the encrypted hash of the attachment, hashing the message, including the indication of the opening of the message the recipient, and the attachment to provide first digital fingerprints of the message, including the indication of the opening of the message at the recipient and the attachments, decrypting the encrypted hash of the message, including the indication of the opening of the message at the recipient, and the attachment to provide second digital fingerprints of the message, including the indication of the opening of the message at the recipient and the attachment, and comparing the first and second digital fingerprints of the message, including the indication of the opening of the message at the recipient, to determine the authenticity of the message, including the indication of the opening of the message at the recipient and first and second fingerprints of the attachment to determine the authenticity of the attachment (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

18. As per claims 10 and 16, Tomkow teaches the system further including the steps at the server of:

indicating to the sender the results of the comparisons, and disposing of the message, including the indication of the opening of the message at the recipient, and the encrypted hash of the message, including the indication of the opening of the

message at the recipient, and the attachment and encrypted hash of the attachment when the message, the attachment and the encrypted hashes are transmitted by the server to the sender (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

19. As per claim 11, Tomkow teaches the system further wherein the server receives the message from the sender through the internet and wherein the server transmits the message to the recipient through the internet and wherein the server re-transmits the message, including the indication of the opening of the message at the recipient, to the recipient through the internet and wherein the server transmits the message through the internet to the sender (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

20. As per claim 12, Tomkow teaches the system further wherein the server indicates the results of the comparison to the sender through the internet and wherein the server disposes of the message, the attachment and the encrypted hashes of the message and the attachment when the message and the encrypted hash are transmitted by the server to the sender through the internet (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

21. As per claim 14, Tomkow teaches the system further including the steps at the server of: receiving the message, the attachment and the encrypted hash of the combination of the message and the attachment from the sender, hashing the

combination of the message and the attachment to provide a first digital fingerprint and decrypting the encrypted hash of the combination of the message and the attachment to form a second digital fingerprint, and determining the authenticity of the message and the attachment on the basis of the first and second digital fingerprints (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7 validation process where the message is received at the server, including where a first and second digital fingerprint of the message are created).

22. As per claims 17, Tomkow teaches the system further wherein the server receives the message from the sender through the internet, the server transmits the message to the recipient through the internet, the server receives the message, including the indication of the opening of the message the recipient, through the internet, and the server transmits the message, including the indication of the opening of the message at the recipient, through the internet to the sender (Tomkow, pg. 9, line 19 to pg. 10, line 3, and fig. 1)

23. As per claims 18, Tomkow teaches the system further wherein the server indicates the results of the comparison to the sender through the internet and wherein the server disposes of the message, including the indication of the opening of the message at the internet, and the encrypted hash of the message, including the indication of the opening of the message, when the message and the encrypted hash

are transmitted by the server to the sender through the internet (Tomkow, see pg. 26, lines 9-30 and pg. 39, lines 2-27 with corresponding fig. 7).

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicholas Taylor whose telephone number is (571) 272-3889. The examiner can normally be reached on Monday-Friday, 8:00am to 5:30pm, with alternating Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/NT/
Nicholas Taylor
Examiner
Art Unit 2141

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2145